WO

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Ryan Galal VanDyck,

Petitioner,

v.

United States of America,

Respondent.

No. CV-21-00399-TUC-CKJ

ORDER

On October 4, 2021, the Petitioner filed a Motion under 28 U.S.C. § 2255 to Vacate, Set Aside, or Correct Sentence by a Person in Federal Custody (Petition). He raises two claims of constitutional error: 1) his trial counsel was ineffective for failing to raise a Fourth Amendment challenge to the police opening an America Online, Inc. (AOL) email attachment without a warrant, and 2) his appellate counsel was ineffective for failing to challenge the extension of a search warrant deadline because it was based on knowingly false statements.

On December 5, 2016, the Court sentenced the Petitioner, Defendant VanDyck, in CR 15-742-TUC-CKJ to concurrent sentences of 240 months imprisonment followed by lifetime supervised release for conspiracy to produce child pornography and 60 months imprisonment followed by lifetime supervised release for possession of child pornography. (Judgment of Commitment (Doc. 175)). Pretrial, the Court denied Petitioner's motion to suppress evidence obtained during a search of his home, including child pornography found

on electronic devices seized during the search. Thereafter, he agreed to a bench trial based on a stipulated record. The Court found him guilty on June 7, 2016.

On direct appeal, the Petitioner argued for the first time that police needed a warrant to open the AOL email attachment, and therefore, that the evidence against him should be suppressed as fruits of this poisonous tree. The appellate court denied relief because it found the Petitioner waived the challenge by failing to raise it at trial. On appeal, he did not challenge the warrant extension. His direct appeal was denied, and his conviction affirmed on July 15, 2019. The Supreme Court denied his petition for *certiorari* on October 5, 2020. He filed his habeas Petition within the one-year statute of limitation period provided under the Effective Death Penalty Act of 1996 (AEDPA). 28 U.S.C. § 23255(f).

A. 28 U.S.C. § 2255: Motion to Vacate or Correct Sentence

Title 28 of the United States Code, Section 2255 provides for collateral review of Petitioner's sentence as follows:

> A prisoner in custody under sentence of a court established by Act of Congress claiming the right to be released upon the ground that the sentence was imposed in violation of the Constitution or law of the United States, or that the court was without jurisdiction to impose such sentence, or that the sentence was in excess of the maximum authorized by law, or is otherwise subject to collateral attack, may move the court which imposed the sentence to vacate, set aside or correct the sentence. A motion for such relief may be made at any time.

28 U.S.C. § 2255.

A district court will summarily dismiss a § 2255 petition "[i]f it plainly appears from the face of the motion and any annexed exhibits and the prior proceedings in the case that the Petitioner is not entitled to relief." Rule 4(b), Rules Governing § 2255 Actions. The district court need not hold an evidentiary hearing when the Petitioner's allegations, viewed against the record, either fail to state a claim for relief or are patently frivolous. *Marrow v. United States*, 772 F.2d 525, 526 (9th Cir. 1985).

Generally, "claims not raised on direct appeal may not be raised on collateral review unless the petitioner shows cause and prejudice." *Massaro v. United States*, 538 U.S. 500, 504 (2003); *see also United States v. Ratigan*, 351 F.3d 957, 962 (9th Cir. 2003) ("A § 2255 movant procedurally defaults his claims by not raising them on direct appeal and

not showing cause and prejudice or actual innocence in response to the default."). Claims of ineffective assistance of counsel are, however, an exception and may be raised on collateral review even if they were not raised on direct appeal. *See Massaro*, 538 U.S. at 504 ("[A]n ineffective-assistance-of-counsel claim may be brought in a collateral proceeding under § 2255, whether the petitioner could have raised the claim on direct appeal."); *United States v. Jackson*, 21 F.4th 1205, 1212 (2022) (ineffective assistance of counsel claims may be brought in collateral proceedings under § 2255.")

B. Ineffective Assistance of Counsel Standard of Review

The Supreme Court enunciated a two-prong standard for judging a criminal defendant's contention that the Constitution requires a conviction to be set aside because counsel's assistance at trial was ineffective in *Strickland v. Washington*, 466 U.S. 668 (1984). First, the defendant must show that, considering all the circumstances, counsel's performance fell below an objective standard of reasonableness. *Id.* at 687-88. To this end, the defendant must identify the acts or omissions that are alleged not to have been the result of reasonable professional judgment. *Id*. at 690. The court must then determine whether, in light of all the circumstances, the identified acts or omissions were outside the wide range of professionally competent assistance. *Id*. at 688-90. Second, the defendant must affirmatively prove prejudice. *Id*. at 691-92. He must show that there is a reasonable probability that, but for counsel's unprofessional errors, the result of the proceeding would have been different. *Id*. at 694. A reasonable probability is a probability sufficient to undermine confidence in the outcome. *Id*.

The court need not address both *Strickland* requirements if the petitioner makes an insufficient showing regarding just one. *Id*. at 697 (explaining: "[i]f it is easier to dispose of an ineffectiveness claim on the ground of lack of sufficient prejudice, ... that course should be followed."); *Rios v. Rocha*, 299 F.3d 796, 805 (9th Cir. 2002) (stating: "[f]ailure to satisfy either prong of the *Strickland* test obviates the need to consider the other.")

C. The Warrant and Warrantless Searches

Both of the ineffective assistance of counsel claims challenge alleged searches by Tucson Police officers that occurred when, without a warrant, police officers opened the email attachment that was sent by AOL to the National Center for Missing and Exploited Children (NCMEC), a private organization, which in turn secured Petitioner's identity and sent a Cybertip report with a copy of the image and notation that it "appears to contain child pornography" to Tucson police. Police opened the email attachment without a warrant based on the third-party doctrine, which provides:

> [A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. [735, 743-44 (1979)]. That remains true "even if the information is revealed on the assumption that it will be used only for a limited purpose." *United States v. Miller*, 425 U.S. 435, 443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). As a result, the Government is typically free to obtain such information from the recipient without triggering Fourth Amendment protections.

Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).

Detective Holewinski obtained a search warrant for Petitioner's home, including any electronic devices based on his affidavit which stated in pertinent part that AOL had made a Cybertip report to NCMEC "in reference to one of its users sending an image depicting child sexual abuse to another email address." The affidavit described the image attached to the email as: "sexually exploitive in nature." Detective Holewinski described the filename 266211007.jpeg as: "an image file of a prepubescent male child who appears to be between 7 and 12 years of age. The boy is wearing a red shirt and is wearing a pair of boxer shorts that are pulled down to his upper thighs. The child is lying back and his erect penis is exposed. The focus of the image is on the child's penis." The affidavit reflects that the police had verified the tip as "in fact" depicting a child in a state of exploitive exhibition" and secured thereafter the comcast subscriber information which reflected the subscriber was a landscape company owned by the Petitioner. The Court accepts Petitioner's argument that information provided in the affidavit, without the description of the email attachment after it was viewed by Holewinski, would not have been enough to

secure the warrant to search Petitioner's home and electronic devices. (Motion at Ex. 3: Warrant and Affidavit (Doc. 1-2) at 44-47.)

The original warrant was to be executed on September 4, 2014. Police amended the warrant based on an affidavit attesting that Petitioner was out of town and would be back in town the week of September 8, 2014. Petitioner argues that he was home on the 4th, therefore, the warrant affidavit falsely stated that he would not be home until the 8th.

D. Ineffective Assistance of Trial Counsel

1. *Carpenter v. United States*, 138 U.S. 2206 (2018): Third Party Doctrine

When an individual intends to preserve something as private, and this expectation of privacy is one that society is prepared to recognize as reasonable, then intrusion into that private sphere by the government is a search under the Fourth Amendment and requires a warrant. *Id.* at 2213. "'[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.'" *Id.* at 2216 (quoting *Smith*, 442 U.S. at 743-44). This is true "'even if the information is revealed on the assumption that it will be used only for a limited purpose.'" *Id.* (quoting *Miller*, 425 U.S. at 443).

During the pendency of his direct appeal, the Supreme Court issued *Carpenter*, upon which Petitioner relies to argue that the third-party doctrine will not support the warrantless search of the email attachment by police. *States v. VanDyck*, 776 F. App'x 495, 496–97 (9th Cir. 2019).

On appeal, this argument was rejected as waived because Petitioner did not present it at trial to this Court. He also argued the Fourth Amendment required a warrant to obtain the subscriber information associated with his IP address. The Ninth Circuit rejected this argument relying on the conclusion in *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008), that internet users have no expectation of privacy in the IP addresses of the websites they visit because "they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information." *United States v. VanDyck*, 776 F. App'x at 496–97 (quoting *Forrester*, 512 F.3d at 510)). The appellate court rejected the notion that *Forrester* must be reconsidered in light of the

Supreme Court's decision in *Carpenter.* The appellate court found the *Carpenter* decision was a "narrow one." "In *Carpenter*, the Court declined to extend the third-party doctrine to cell site records"; "an individual maintain[s] a 'legitimate expectation of privacy in the record of his physical movements as captured' through cell site records." *VanDyck,* 776 F. App'x at 496 (quoting *Carpenter*, 138 U.S. at 2217)). On direct appeal, the Ninth Circuit declined to extend *Carpenter* beyond cell site records to subscriber information associated with an IP address. This Court does the same. For the reasons explained below, *Carpenter* does not apply to the email attachment that was an image of child pornography.

In *Carpenter,* the government asked the Supreme Court to find that the third-party doctrine applied to cell-site records compiled by a wireless carrier. This digital data tracks a person's movement and is compiled by the carrier for its own business purposes, including finding weak spots in their network and applying roaming charges when another carrier routes data through its cell sites or selling aggregated location records to data brokers, etc. Cell phones continuously generate this data by scanning their environment looking for the best signal from the closest site and tap into the wireless network several times a minute whenever the phone signal is on, even if the cell phone is not in use by the subscriber. Without a warrant, law enforcement obtained cell site records for Carpenter's cell phone for a four-month period which showed he was near four of the charged robbery locations. The trial court, affirmed on appeal, denied suppression of the cell site data because he shared the information with a third-party, his wireless carrier. *Carpenter,* 138 S.Ct. at 2212.

The Supreme Court reversed. It rejected application of cases addressing a person's expectation of privacy in information voluntarily turned over to third parties like *United States v. Miller,* 425 U.S. 435 (finding no expectation of privacy in bank's financial records for Miller) and *Smith v. Maryland,* 442 U.S. 735 (finding no expectation of privacy in dialed telephone numbers compiled by the telephone company to route phone calls). Instead, the Court followed *United States v. Jones,* 565 U.S. 400, which concluded that privacy concerns are raised by GPS tracking because it obtains the whole of a person's

physical movements. The distinction between the two being two-fold: 1) the nature of the document or information sought and 2) the act of sharing. In *Jones*, the nature of the protected interest was the extremely personal compilation or a person's every movement as compared to minimal personal interests in *Smith and Miller* where third-party business records were compiled by the businesses for their own business purposes. *Carpenter*, 138 S. Ct. at 2217-2221. Comparatively, agents surreptitiously installed and activated a GPS devise on Jones' vehicle, but Miller voluntarily revealed his affairs to the bank by using checks, deposit slips, and bank statements, and Smith voluntarily conveyed numbers to the phone company as he dialed them. *Id.* at 2215-2216.

In dissent, justices criticized *Miller* and *Smith,* explaining they are limited such as when the government obtains the modern-day equivalents of an individual's own papers or effects even if held by a third party. *Carpenter,* 138 S.Ct at 2230 (Justice Kennedy, dissenting, joined by Justices Thomas and Alito) (citing *United States v. Warshak,* 631 F.3d 266, 283-88 (6th Cir. 2010) (emails held by Internet service provider are like letters held by a mail carrier, *Ex parte Jackson,* 96 U.S. 727, 733 (1878)). Concluding, "whatever may be left of *Smith* and *Miller,* few doubt that e-mail should be treated much like the traditional mail it has largely supplanted—as a bailment in which the owner retains a vital and protected legal interest." *Carpenter,* 138 S.Ct at 2270 (Justice Gorsuch, dissenting). The Petitioner urges this Court to follow this line of reasoning and find police officers trespassed into a constitutionally protected space when they opened his email without a warrant and/or that the email is constitutionally protected property, like a piece of mail. (Reply (Doc. 20) at 12-18); *Ex parte Jackson,* 96 U.S. 727, 733 (1878) (finding individual's own papers include letters held by mail carrier).

In Petitioner's case, however, law enforcement did not intrude into his email accounts at all. AOL occasioned the intrusion and then turned the email information over to NCMEC, which transmitted the Cybertip report and a copy of the email attachment to law enforcement. Law enforcement viewed a copy of the email attachment. The

government did not inspect any private area of any electronic device until it obtained a warrant. There was simply no warrantless physical trespass into Petitioner's property.

After *Carpenter*, the third-party doctrine remains. *Miller* and *Smith* remain good law, albeit the third-party doctrine has been narrowed. The Court finds that *Carpenter* does not apply to preclude application of *Smith* and *Miller* to the facts of this case which are distinguishable from *Jones* and *Carpenter*. While the dissent discounted *Miller* and *Smith*, the majority rejected a singular property-based approach to the Fourth Amendment. According to the majority in *Carpenter*, *Jones* "breathed new life" into the property based Fourth Amendment's roots in common-law trespass. *Carpenter*, 138 S.Ct. at 2213. There, the inquiry is whether a state actor physically intruded into private property "for the purpose of obtaining information." *Jones*, 565 U.S. at 404-405. If "the Government obtains information by physically intruding on persons, houses, papers, or effects, a search within the original meaning of the Fourth Amendment has undoubtedly occurred." *United States v. Thomas*, 726 F.3d 1086, 1092 (9th Cir. 2013) (cleaned up).

"The Fourth Amendment indicates with some precision the places and things encompassed by its protections: persons, houses, papers, and effects." *Florida v. Jardines*, 569 U.S. 1, 6 (2013). In *Jones*, the Supreme Court made it clear that the trespassory-focus it renewed, only extended to searches of "those items ('persons, houses, papers, and effects') that [the Fourth Amendment] enumerates." *Jones*, 565 U.S. at 411 n.8; *see also Patel v. City of Montclair*, 798 F.3d 895, 898 (9th Cir. 2015) (adopting this understanding of *Jones*). In other words, the authority issued after *Jones* makes it clear that "*Jones* establishes a default rule that a government intrusion with respect to the enumerated items of the Fourth Amendment, regardless of a defendant's reasonable expectation of privacy, will implicate the constitutional protection against unreasonable searches and seizures" while "*Katz* [*v. United States*, 389 U.S. 347 (1967)] broadens the reach of the Fourth Amendment beyond the enumerated areas to those areas where the defendant manifests a reasonable expectation of privacy." *Patel*, 798 F.3d at 900.

The majority approach in *Carpenter*, finding that the third-party doctrine did not apply to defeat *Carpenter's* reasonable expectation of privacy, 138 S.Ct. at 2211–19, assumed a search under the Fourth Amendment pursuant to the *Katz* twofold requirement: "first that a person [has] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Katz*, 389 U.S. at 361 (Justice Harlan concurring).[1] *Compare Riley v. California*, 573 U.S. 373, 378–403 (2014) (analyzing the warrantless inspection of cell phone data in terms of *Katz* privacy expectations, not *Jones* property intrusions) *with Florida v. Jardinas*, 569 U.S. 1, 11–12 (2013) (applying *Jones*, with focus on government's physical occupation of tangible thing, like vehicle, house, or its curtilage); *United States v. Dixon*, 984 F.3d 814, 816 (9th Cir. 2020) (same). This is the relevant approach here.

2. *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021): Private Search Exception

The Fourth Amendment protects individuals from government intrusions, not private ones; a private party may conduct a search that would be unconstitutional if conducted by the government. The private search exception to the Fourth Amendment warrant requirement applies in circumstances where a private party's intrusions would have constituted a search had the government conducted it, and the material discovered by the private party then comes into the government's possession. *Id.* at 967-971. Then, law enforcement need not "avert their eyes." *Id.* at 967 (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 489 (1971)).

During the pendency of this Petition, the Ninth Circuit decided *Wilson*, which considered facts very similar to those presented in this case. *See* (Response (Doc. 10) at 14 n. 5) (asserting it was wrongly decided)). In *Wilson*, the court concluded that police violated

[1] "[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. *See Lewis v. United States*, 385 U.S. 206, 210 (1966); *United States v. Lee*, 274 U.S. 559 (1927). But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected. *See Rios v. United States*, 364 U.S. 253 (1960); *Ex parte Jackson*, 96 U.S. 727, 733 (1877)." *Katz v. United States*, 389 U.S. 347, 351-52 (1967).

the Fourth Amendment by opening an email containing child pornography without a warrant based on a Cybertip report to NCMEC from Google. In *Wilson*, the court assumed the agent's review of Wilson's email attachments was a search within the meaning of the Fourth Amendment. *Wilson*, 13 F.4th at 967. The court considered whether "[the agent] was permitted to look at [Wilson's] email attachments under the private search exception, such that the Fourth Amendment did not require him to procure a warrant." *Id.*

Finding the private search exception to be narrow with limited application, the court concluded "an antecedent private search excuses the government from obtaining a warrant to repeat the search but only when the government search does not exceed the scope of the private one." *Id.* at 968. The test is "the degree to which they [the government] exceeded the scope of the private search." *Id.* (citing *Jacobsen*, 466 U.S. 109, 115(1984)).

In *Wilson*, the court concluded the private search doctrine did not except the email search from Fourth Amendment warrant protections because the government's search exceeded the scope of the antecedent private search by Google. Like the Cybertip report of Petitioner's email, Google's Cybertip report of Wilson's email was based on an automated assessment that the images defendant uploaded were the same as images other provider employees had earlier viewed and classified as child pornography; no employee from Google viewed the actual email attachment image. The government's search exceeded this scope because agents actually viewed the image, allowing them to determine exactly what the images showed and to learn that the images were in fact child pornography. *Wilson*, 13 F.4th at 973-974. The "government learned new, critical information that it used to obtain a warrant and then to prosecute defendant for possession and distribution of child pornography." *Id.* at 972.

The court described the "gulf" between Google's hash-tag repository of images sorting illicit images into one of four generic labels, including the A1 classification for images depicting a sex act involving a prepubescent minor. *Id.* at 972. Here, the gulf is arguably wider between the exacting graphic description of the image in the warrant to search the Petitioner's electronic devices and the Cybertip report from AOL, which simply

described that the email "appears to contain child pornography." Because no one at Google had looked at the images, "any privacy interest in those images had [not] been extinguished; the Google algorithm "'frustrated [Wilson's] [privacy] expectation in part,' but it 'did not . . . strip the remaining unfrustrated portion of that expectation of all Fourth Amendment protection.'" *Id.* at 976.

Under *Wilson*, the record in Petitioner's case would support suppression of the evidence gathered pursuant to the warrantless search of the email attachment, and further suppression of all the evidence found pursuant to the warrant to search his electronic devices because that warrant was based on the fruit of the poisonous tree, the warrantless search of the email image. *Wilson*, however, does not answer the question of whether reviewing email attachments is a search within the meaning of the Fourth Amendment because in *Wilson*, the parties and the court assumed opening the email without a warrant was a search. *Id.* at 967.

Here, the government makes no such concession. Respondent argues that under the AOL terms of service and privacy policy, the Petitioner knew that his email attachments were subject to monitoring by AOL and disclosure to law enforcement. In other words, Petitioner did not have a reasonable expectation in the privacy of the email attachments, especially there was no reasonable expectation in privacy in email attachments that contain child pornography. The Government does not need to invoke the private search exception, unless inspection by law enforcement of the email attachment was a search for Fourth Amendment purposes.

3. Fourth Amendment Search: Reasonable Expectation of Privacy

A Fourth Amendment "search" occurs when the government invades a person's "reasonable expectation of privacy." *Jones*, 565 U.S. at 404 (quoting *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)). Whereas the government carries the burden to establish the private search exception, the burden is on the Petitioner to demonstrate that he had a reasonable expectation of privacy in the area searched. *United States v. Sarkisian*, 197 F.3d 966, 986 (9th Cir. 1999); *United States v. Nerber*, 222 F.3d

597, 599 (9th Cir. 2000). Standing is a threshold issue, and the Court will not proceed with a Fourth Amendment analysis unless the Petitioner can establish standing[2] to contest the search. *United States v. Singleton*, 987 F.2d 1444, 1449 (9th Cir. 1993). A reasonable expectation of privacy exists if: (1) "the individual manifested a subjective expectation of privacy in the object of the challenged search?" and (2) "society is willing to recognize that expectation as reasonable?" *California v. Ciraolo*, 476 U.S. 207, 211 (1986); *Rakas v. Illinois*, 439 U.S. 128, 143–44 (1978). This two-prong test reflects that the privacy interest is both subjective and objective. *United States v. Ford*, 34 F.3d 992, 995 (11th Cir. 1978). In other words, Petitioner must show he subjectively expected his email attachment was private and that this expectation was reasonable.

In 2014, AOL's email service required a user account to be opened pursuant to a subscriber consent agreement, including the AOL terms of service and privacy policy. By clicking "Sign Up" the subscriber acknowledged receipt of the terms of service, and there were hyperlinks to both the terms of service and privacy policy. (Response (Doc. 10) at 2-3 (citing Exhibit A: Create Account)).

The terms required the following: "[compliance] with applicable laws and regulations and not participate in, facilitate, or further illegal activities"; forbade the user from "post[ing] content that contains explicit or graphic descriptions or accounts of sexual acts or is threatening, abusive, harassing, defamatory, libelous, deceptive, fraudulent, invasive of another's privacy, or tortious." The terms included: notice that to "prevent violations and enforce [the terms] and remediate any violations," AOL reserved the right to "take any technical, legal, and other actions that we deem, in our sole discretion, necessary and appropriate without notice to [the user]." *Id.* at 3 (quoting Ex. B: Terms of Service).

---

[2] To establish standing to challenge the legality of a search or seizure, a defendant must demonstrate that he or she has a "legitimate expectation of privacy" in the items seized or the area searched. *United States v. Padilla*, 508 U.S. 77, 82 (1993) (*per curiam*) (Padilla I); *Rakas v. Illinois*, 439 U.S. 128, 143 (1978) The proponent of a motion to suppress has the burden of establishing that his own Fourth Amendment rights were violated by the challenged search or seizure." *Rakas v. Illinois*, 439 U.S. 128, 132 n.1 (1978), *abrogated in part on other grounds by Minnesota v. Carter*, 525 U.S. 83 (1998).

The terms of service incorporated the separate AOL privacy policy, including: AOL "may use information about [the user's] use of certain communication tools (for example, AOL e-mail or AOL Instant Messenger)"; "AOL does not read [the user's] private online communications without [the user's] consent," although "[t]he contents of the user's] online communications, as well as other information about [the user] as an AOL user, may be accessed and disclosed" where "AOL has a good faith belief that a crime has been or is being committed by an AOL user . . .." *Id.* (quoting Ex. C: Privacy Policy)

In summary, the terms of service expressly precluded use of AOL email to send illegal attachments, which includes child pornography. Petitioner was expressly warned that AOL could "take any technical, legal, and other actions" that it deemed necessary and appropriate. Additionally, the privacy policy confirmed that even if AOL did not read the text of emails, it monitored the contents of emails and attachments and would disclose illegal material to law enforcement. The Court agrees with the Respondent that the Petitioner's use of AOL email, under the terms of service and privacy policy, is factually inconsistent with a manifestation of a subjective expectation of privacy. The Petitioner's assertion of a subjective expectation in privacy is especially suspect because he included in the subject line the directive: "please trade." (Reply, Ex. 1: Supp. Motion to Suppress (Doc. 20-1) at 1.)

This is not a case like *Wilson* where the Court may determine whether a person's reasonable privacy expectations have been reduced or compromised. Like all Fourth Amendment cases, the Court must make the threshold assessment of whether inspection by law enforcement of the email attachment was a search for Fourth Amendment purposes.

The Court finds that generally a person may have a reasonable expectation of privacy in his or her emails and email attachments, but that is not the dispositive question. Instead, the Court must determine whether any expectation of privacy was reasonable in relation to this email attachment, which specifically was an image of child pornography that Petitioner sent to another person under the subject heading of "please trade." If the Court assumes Petitioner manifested a subjective expectation of privacy in the email

attachment, even in the face of the evidence cited above suggesting the contrary, this same evidence goes a long way to defeat his claim under the objective prong of the Fourth Amendment analysis. *Compare*: *United States v. Chavez*, 423 F. Supp. 3d 194, 201–06 (W.D. N.C. 2019) (defendant has subjective expectation of privacy in information on Facebook account he attempted "to exclude the public" from seeing and that expectation is objectively reasonable) *with United States v. Meregildo*, 883 F. Supp. 2d 523, 525–26 (S.D. N.Y. 2012) (no expectation of privacy in Facebook posts shared with "friends"); *United States v. Khan*, 2017 WL 2362572, *8 (N.D. Ill. 2017) (no expectation of privacy in Facebook account not invoking any privacy settings); *United States v. Westley*, 2018 WL 3448161, *5–6 (D. Conn. 2018) (same).

"Relevant here, a reasonable person's 'privacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that the systems administrators may monitor communications transmitted by the user.'" (Response (Doc. 10) at 11 (quoting *United States v. Heckenkamp*, 482 F.3d 1142, 1147 (9th Cir. 2007) (finding an objective reasonable expectation in privacy when student attached his computer to university server because university did not announce monitoring, but finding special needs exception to warrant requirement)). *See United States v. Morel*, 922 F.3d 1, 10 (1st Cir. 2019) (applying the third-party doctrine, post-*Carpenter*, finding no reasonable expectation of privacy in photos uploaded to a photo-sharing service called Imgur), *United States v. Ackerman*, 296 F. Supp. 3d 1267, 1272 (D. Kan. 2017) (holding no reasonable objective expectation of privacy" in email attachment containing child pornography in light of the terms of service stating AOL monitored emails and would take legal action if it discovered illegal material), aff'd on other grounds, 804 F. App'x 900, 903 (10th Cir.) (mem. decision), cert. denied, 141 S. Ct. 458 (2020)).

Courts universally find a subscriber does not maintain a reasonable expectation of privacy with respect to subscriber information because: 1) there is a distinction between content of electronic communications, which is protected, and non-content information,

like a subscriber's screen name and screen identity, which is not;[3] 2) the language of the Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. 2701 et seq.,[4] expressly permits ISPs to disclose subscriber information to non-governmental third parties and also to the government under certain restrictive conditions, and 3) subscriber agreements with the internet service providers (ISPs) usually expressly provide for this disclosure. These factors cut in favor of finding a subscriber's subjective expectation of privacy in his or her non-content information as being one that society would not be willing to accept as objectively reasonable. *Freedom v. Am. Online, Inc.*, 412 F.Supp.2d 174, 181-83 (Conn. 2005) (citing *United States v. Hambrick*, 55 F.Supp.2d 504 (W.D.Va.1999), aff'd 225 F.3d 656 (4th Cir.2000) (rejecting fruit of the poisonous tree argument related to IPS compliance with government subpoena by IPS providing defendant's name and fact that he was connected to Internet at IP address because society would not accept such a privacy interest); *United States v. Kennedy*, 81 F.Supp.2d 1103 (D.Kan.2000) (same). As explained in *Hambrick,* objective reasonableness is a value judgment and a determination of how

[3] *See*: *Smith*, 442 U.S. at 741 (distinguishing listening devices that acquire contents of communication from pen registers that do not); *Forrester*, 512 F.3d at 509–12 (finding a computer user has no legitimate expectation of privacy in the to/from addresses of email messages sent from, and the internet protocol ("IP") addresses visited by, a defendant on his home computer); *see also: In Ex parte Jackson*, 96 U.S. at 732–33 (distinguishing Fourth Amendment protection for contents of sealed envelopes even when turned over the third party mail carrier does not extend to address and other information disclosed on face of the envelope); *Lustiger v. United State*s, 386 F.2d 132, 139 (9th Cir. 1967) (same), *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001) (finding homeowner's reasonable expectation of privacy in home and belongings, including computer; asserting that "Users would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting. [citation omitted].) They would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient; at this moment, the e-mailer would be analogous to a letter-writer, whose expectation of privacy ordinarily terminates upon delivery of the letter.")

[4] Congress enacted the Electronic Communications Privacy Act of 1986 protecting against the unauthorized interception of various forms of electronic communications and updating federal privacy protections and standards given changes in computer and telecommunications technologies. Title I of the Act addresses interception of wire, oral and electronic communications. Title II addresses access to stored wire and electronic communications and transactional records. Title III addresses pen registers and trap and trace devices. *Hambrick*, 55 F. Supp. 2d at 507. Hambrick challenged Title II. Petitioner's case falls under Title I.

much privacy we should have as a society under certain circumstances. *Hambrick*, 55 F. Supp.2d at 506.

Here, Petitioner was not an anonymous actor. He agreed to AOL's terms of service and privacy policy making him aware that AOL was monitoring his email attachments and could disclose them to law enforcement if they involved illegal conduct, including child pornography. He knew his email was not private. He intentionally and knowingly attached an illegal image of child pornography to an email he knew was monitored by AOL and subject to disclosure to law enforcement. He shared it with another person without any restriction placed on its use, such as marking the email confidential. Instead, in the subject line, an area subject to view without opening the email, he invited sharing: "please trade." These facts cut against society accepting Petitioner's subjective belief in the privacy of the email attachment as being a reasonable expectation. This is consistent with finding any privacy expectation Petitioner may have had in the email attachment has been reduced under *Heckenkamp* or that there is no reasonable expectation of privacy based on the third-party doctrine.

Society has strong public policy in favor of protecting children against acts of sexual abuse. *C.J.C. v. Corp. of Cath. Bishop of Yakima*, 138 Wash. 2d 699, 726, 985 P.2d 262, 276 (1999), as amended (Sept. 8, 1999). In that interest, Congress can prohibit the display of materials that are harmful to minors. *Ginsberg v. New York*, 390 U.S. 629 (1968), including protecting children from exposure to sexually explicit material, *Reno v. Am. C.L. Union*, 521 U.S. 844, 875 (1997). Two federal statutes, the Stored Communications Act and the Protect Our Children Act, in combination create a statutory scheme placing legal reporting obligations on Internet Service Providers (ISPs)[5], like AOL.

The Stored Communications Act (SCA)[6] criminalizes unauthorized searches of stored electronic communications content, 18 U.S.C. § 2701(a)–(b), but expressly excepts electronic communication service providers (ESPs)[7] from liability. *Id.* § 2701(c)(1). This

[5] *See* n. 7.
[6] SCA was enacted as Title I of the Electronic communications ACT (ECPA)
[7] An ISP is an electronic communications service provider (ESP).

exception is necessary to enable ESPs to ensure that user content does not violate the ESPs' own terms of use. Because the Stored Communications Act does not authorize ESPs to do anything more than access information already contained on *their* servers as dictated by their terms of service, ESPs may conduct warrantless searches. The Protect Our Children Act requires these private parties, including AOL, to report evidence derived from those searches to a government agent or entity, 18 U.S.C. § 2258A. The Protect Our Children Act disclaims any governmental mandate to search and provides that this statute "shall [not] be construed to require" a "provider"[8] to "monitor" users or their content or "affirmatively search, screen, or scan for" evidence of criminal activity. 18 U.S.C. § 2258A(f). In this way, searches are at the discretion of the provider and done for its own business interests in keeping child pornography and exploitation off their platforms; there is a direct financial interest in keeping child pornography off platforms to not lose advertising opportunities or be blocked from app stores. *Cf.*, *United States v. Rosenow*, 50 F.4th 715, 729–31 (9th Cir. 2022) (finding as matter of first impression that these federal laws do not transform ESP private searches into government action).

In *Wilson*, the Court described the statutory reporting responsibility as follows: "[i]n order to reduce ... and ... prevent the online sexual exploitation of children," such providers," . . . "as soon as reasonably possible after obtaining actual knowledge" of "any facts or circumstances from which there is an apparent violation of ... child pornography [statutes]," must "mak[e] a report of such facts or circumstances" to NCMEC. 18 U.S.C. § 2258A(a). NCMEC adds subscriber details and forwards a CyberTip report to the appropriate law enforcement agency for possible investigation. *Id.* at §§ 2258A(a)(1)(B)(ii), (c). This statutory scheme, especially the Protect Our Children Act, reflects society's determination that internet communications that appear to violate child pornography statutes should not be private in the context of the Fourth Amendment. In other words, government intrusion to protect our children from sexual exploitation is not

[8] 2018 Amendments, Pub.L. 115-395 § 2(7)(A) (stuck out "an electronic communication service provider or a remote computing service provider" and inserted "a provider."

an infringement on a legitimate privacy interest; child pornography is not a personal or societal value protected by the Fourth Amendment.

The factors identified in the cases finding no reasonable expectation of privacy in subscriber information are all met here, except the email attachment is content. Therefore, *Forrester*,[9] wherein the Ninth Circuit determined there is no legitimate expectation of privacy in subscriber information, the to/from addresses of email messages, and the internet protocol (IP) addresses visited by the user, is distinguishable.

"Determining whether society would view the expectation of privacy as objectively reasonable turns on whether the government's intrusion infringes on a legitimate interest, based on the values that the Fourth Amendment protects." *California v. Ciraolo,* 476 U.S. 207, 212 (1986) "'[T]he test of legitimacy is not whether the individual chooses to conceal assertedly 'private activity,' but instead is whether the government's intrusion infringes upon the personal and societal values protected by the Fourth Amendment.'" *Id.* (quoting *Oliver v. United States*, 466 U.S. 170, 182-83 (1984)). "No single factor determines whether an individual legitimately may claim under the Fourth Amendment that a place should be free of government intrusion, but courts give weight to such factors as the "intention of the Framers of the Fourth Amendment, the uses to which the individual has put a location, and our societal understanding that certain areas deserve the most scrupulous protection from government invasion." *Oliver,* 466 U.S. at 177-178. "Official conduct that does not 'compromise any legitimate interest in privacy' is not a search subject to the Fourth Amendment." *Illinois v. Caballes,* 543 U.S. 405, 408 (2005) (quoting *Jacobsen*, 466 U.S. at 123).

In *United States v. Place,* 462 U.S. 696 (1983), the Supreme Court held a "canine sniff" by a drug-sniffing dog was not a search within the meaning of the Fourth Amendment. 462 U.S. at 707. In *Place,* law enforcement seized luggage from a passenger

[9] *See Supra* at 5 (quoting *VanDyck*, 776 F. App'x at 496–97 (quoting *Forrester*, 512 F.3d at 510)) (explaining internet users "should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.")

and took it to another location where a drug-sniffing dog alerted officers that drugs were in the luggage; officers obtained a warrant to search the luggage and found cocaine. *Id.* at 699. Recognizing a reasonable expectation in privacy in the contents of personal luggage, the Court held the dog's sniff test was not a Fourth Amendment search and emphasized the unique nature of the investigative technique, which could identify only criminal activity. The Court reasoned that a "canine sniff" by a well-trained narcotics detection dog, does not require opening the luggage and does not expose noncontraband items that otherwise would remain hidden from public view, as compared to an officer looking through the contents of the luggage. The manner of the investigation being much less intrusive than a typical search and the disclosure reflecting only the presence or absence of narcotics, a contraband item, the Court found the canine sniff is "*sui generis;*" it discovers nothing uniquely personal. The Court noted: "We are aware of no other investigative procedure that is so limited both in the manner in which the information is obtained and in the content of the information revealed by the procedure. . . . -- exposure of respondent's luggage, which was located in a public place, to a trained canine -- did not constitute a "search" within the meaning of the Fourth Amendment." *Place*, 462 U.S. at 707.

In *United States v. Jacobsen*, the Supreme Court extended *Place* to the chemical field test of a white powdery substance to reveal that the substance was cocaine. 466 U.S. at 122-24. Federal Express employees opened a damaged package to discover zip-lock plastic bags containing a white powder, called law enforcement, and repacked the contents in the original packaging before officers arrived, who then removed the plastic bags from the broken package, opened them, and field-tested the white powder, identifying it as cocaine. *Id.* at 111-12. The Supreme Court held that removal of the plastic bags from the tube and the agent's visual inspection was not a Fourth Amendment violation because agents learned nothing that had not previously been learned during the private search, *id.* at 120, but noted it remained to be determined whether the additional intrusion occasioned by the field test, which had not been conducted by the Federal Express employees, exceeded the scope of the private search and was, therefore, an unlawful "search" within

the meaning of the Fourth Amendment, *id.* at 122. This finding was relied on in *Wilson* and discussed above in the context of applying the private search exception to Fourth Amendment searches. *See supra.* at 10.

Relying on *Place*, the Court in *Jacobsen* concluded that the additional digital scan of the white substance was not a Fourth Amendment search, because the test disclosed only whether the substance was cocaine and "nothing [else]," . . . "not even whether the substance was sugar or talcum powder." Turning first to determine whether this was a search subject to the Fourth Amendment, the Court asked, "whether it infringed an expectation of privacy that society is prepared to consider reasonable?" *Id.* at 122.

The Court found a chemical test that merely discloses whether a particular substance is cocaine does not compromise any legitimate interest in privacy. It hinged this conclusion on the fact that virtually all field tests conducted under comparable circumstances will result in positive drug findings, but the conclusion did not dependent on the test results. Even if the test were negative, no legitimate privacy interest has been compromised. The Court explained that "Congress has decided-and there is no question about its power to do so--to treat the interest in 'privately' possessing cocaine as illegitimate; thus, governmental conduct that can reveal whether a substance is cocaine, and no other arguably 'private' fact, compromises no legitimate privacy interest." *Id.* at 123.

Here, Congress has done the same. With passage of the Protect Our Children Act, Congress has treated the interest in privately possessing child pornography as illegitimate. The government's conduct at issue in this case can only reveal whether an image is child pornography. No other private fact is revealed when the government opens an image reported to it in a Cybertip. While the Court in *Place* could not imagine another investigative procedure more limited both in the manner that information is obtained and in the content of the information revealed by a procedure, those at issue here are such. A private party, AOL, reviewed, monitored, and reported the email attachment pursuant to terms of service and privacy policies that Petitioner expressly agreed applied to his use of AOL email. Law enforcement received a Cybertip pursuant to a reliable hashtag system

designed by EPS companies to identify child pornography by designated category. It was a virtual certainty that the image attached to the Cybertip report was illegal child pornography. There was nothing uniquely private about the copy of the email attachment included in the Cybertip report that law enforcement officers opened. Officers did not have access to and did not open the Petitioner's email or look in any areas of his computer or other electronic devices.

This Court concludes that society has decided the interest in "privately" possessing child pornography is illegitimate. Opening the image attached to the Cybertip report did not infringe an expectation of privacy that society is prepared to consider reasonable. Opening the copy of the image of child pornography included in the Cybertip report was not a search within the meaning of the Fourth Amendment.

Importantly, the context of this Court's inquiry is whether Petitioner's trial counsel was ineffective, i.e., whether counsel's performance fell below an objective standard of reasonableness. To assesses the merits of Petitioner's assertion that his trial counsel should have raised a Fourth Amendment challenge to the warrantless search of the AOL email attachment, the Court must determine whether, in light of all the circumstances, this omission was outside the wide range of professionally competent assistance, and if so, whether this prejudiced the result of the trial proceeding. Even with the advantage of *Carpenter* and *Wilson*, the claim fails on the merits. The Petitioner cannot establish prejudice because he cannot show a reasonable probability that he would have prevailed with a motion to suppress and would not have been convicted, if trial counsel had challenged the warrantless opening of the email attachment in the Cybertip report.

In 2014, trial counsel could reasonably have concluded that this challenge would not succeed because it was not a search for purposes of the Fourth Amendment based on the third-party doctrine or AOL's subscriber agreement, or that if there was a search, the private search exception applied. In short, trial counsel could reasonably have concluded the claim lacked merit. Even if not entirely meritless, the claim's viability was sufficiently doubtful to permit a reasonable attorney to omit it in favor of other better arguments. *See*

Miller v. Keeney, 882 F.2d 1428, 1434 (9th Cir. 1989) (holding not ineffective assistance of counsel claim that was not frivolous but would not have led to reasonable probability of reversal). Trial counsel filed two motions to suppress raising multiple challenges, therefore, the Court concludes that he exercised professional discretion to omit this claim. *See Smith v. Murray*, 477 U.S. 527, 536 (1986) ("winnowing out weaker arguments on appeal and focusing on those more likely to prevail, . . . is the hallmark of effective appellate advocacy." (quoting *Jones v. Barnes*, 463 U.S. 745, 751–52 (1983)). The Court finds that the decision to not raise this claim did not fall "below an objective standard of reasonableness" and was not outside the range of competence demanded of attorneys in criminal cases." *Strickland*, 466 U.S. at 687.

E. Ineffective Assistance of Appellate Counsel

Petitioner claims his appellate counsel was ineffective for failing to assert this Court erred when it rejected his argument that the amended warrant extending the deadline for execution was based on a knowingly false statement. This claim arose because the original warrant provided for police to execute it by September 4, 2014, but when police found out Petitioner was not at home, they sought an amended warrant which extended the execution date to September 9, 2014. The affidavit for the amendment provided that "Before the warrant was served, detectives found out that one of the residents of the home was out of town. This resident, Ryan VanDyck, has previously been investigated in crimes relating to child pornography and inappropriate relationship with a minor child. Ryan VanDyck will be back in town the week on 9/8/14." (Motion, Ex. 4: Amended Warrant (Doc. 1-2) at 49.) Petitioner argued that he returned home on September 4, 2014. After hearing testimony, this Court found officers had a good faith basis for the statements made in the affidavit.

At the suppression hearing, police attested they generally executed search warrants on Thursday because that was when both officers were usually available. September 4 was a Thursday. Police became aware through Petitioner's wife, by use of "a ruse," that Petitioner would not be home that day. Police also surveilled his home on that day and did not see him there. The following Monday, September 8, police sought the amendment

supported by the affidavit attesting the Petitioner would be back in town the week on September 8, 2014, requesting to serve the warrant on the ninth. (Response (Doc. 10) at 5 (citing Excerpts of Record (ER) 128-231, 169)).

The Court assumes that the Petitioner returned home on the 4th as reflected in his travel itinerary, but he would not have been home before 4p.m. State law, A.R.S. § 13-3917 prohibits executing search warrants at night, defined as after 6:30p.m., without a judicial finding of good cause. When police sought the amendment, they were not privy to Petitioner's travel itinerary, except they were told by his wife that he was out of town until September 4, and they did not seem him at home that day. This Court finds no false statements in the affidavit, but there is an omission of the fact that, according to Petitioner's wife, he would be home on the fifth. The Court notes that the fifth was beyond the original warrant's execution deadline., therefore, an extension was required. Instead, of seeking the amendment on Friday, police waited until Monday, September 8, 2014. So what?

While the Court found Petitioner's ineffective assistance of trial counsel claim to be extremely weak, his claim of ineffective assistance of appellate counsel is frivolous, especially when considering the standard of review. When a magistrate judge issues a warrant, the reviewing court will usually not second guess the finding of probable cause. *United States v. Leon*, 468 U.S. 897, 913–14 (1984). Issuance of a search warrant carries "a presumption of validity with respect to the affidavit supporting the search warrant," *Franks v. Delaware*, 438 U.S. 154, 171 (1978), except if the magistrate relied on false statements that the affiant made knowingly or recklessly, *Leon*, 468 U.S. at 154. Then, suppression may remedy a warrant that lacked probable cause, if Petitioner can establish, by a preponderance of the evidence, the following: (1) the affiant officer intentionally or recklessly made false or misleading statements or omissions in support of the warrant, and (2) the false or misleading statement or omission was material, i.e., necessary to finding probable cause." *United States v. Norris*, 942 F.3d 902, 909–10 (9th Cir. 2019).

This Court finds no reason to revise the finding made after the *Franks* hearing that the warrant extension application did not contain any knowingly false statements. More

importantly, this Court affirms its earlier finding that the alleged omission was not material to the issuance of the search warrant. Materiality turns on whether any alleged misrepresentations affected the magistrate's determination of probable cause. *Franks*, 438 U.S. at 172. The accepted litmus test for a *Franks* motion is whether probable cause remains once any misrepresentations are corrected, and any omissions are supplemented. *Norris*, 942 F.3d at 910. Here, Petitioner argued that the representation was the but-for cause of the magistrate's decision to grant the warrant extension, but any alleged false statements relevant to extending the time to execute the warrant did not materially affect the probable cause determination. *Norris*, 942 F.3d at 910.

Appellate counsel could not have shown this Court's good faith finding was clearly erroneous or that there was a material omission in the affidavit, therefore, an appellate challenge would have been meritless. As such, appellate defense counsel did not perform deficiently by exercising discretion not to raise a meritless claim. *See Wildman v. Johnson*, 261 F.3d 832, 840 (9th Cir. 2001) ("[A]ppellate counsel's failure to raise issues on direct appeal does not constitute ineffective assistance when appeal would not have provided grounds for reversal."). As noted above, the fact that appellate counsel raised a number of other Fourth Amendment arguments further supports that he carefully reviewed the record and issues and exercised discretion to not raise arguments that would be futile. *See Pollard v. White*, 119 F.3d 1430, 1435 (9th Cir. 1997) (observing that "[a] hallmark of effective appellate counsel is the ability to weed out claims that have no likelihood of success, instead of throwing in a kitchen sink full of arguments with the hope that some argument will persuade the court").

F. Conclusion

In short, this Court's finding that both these claims lack of merit means that the omission of these claims could not have reasonably resulted in reversal on appeal. *See Moormann*, 628 F.3d at 1107 (finding that appellate counsel's omission of a meritless claim meant counsel's performance was not deficient and no prejudice resulted). Petitioner has not established ineffective assistance of trial or appellate counsel under *Strickland.*

Accordingly,

IT IS ORDERED that Petitioner's "Motion to Vacate Sentence or Correct Sentence (Doc. 272)," pursuant to 28 U.S.C. § 2255, filed in CR 15-742-TUC-CKJ and (Doc. 1) filed in CV 21-399-TUC-CKJ is DENIED.

IT IS FURTHER ORDERED that Civil case number CV 22-399-TUC-CKJ is DISMISSED with prejudice.

IT IS FURTHER ORDERED that the Clerk of the Court shall enter judgment accordingly and close this case.

IT IS FURTHER ORDERED that, pursuant to Rule 11(a) of the Rules Governing Section 2254 Cases, in the event Petitioner files an appeal, the Court issues a certificate of appealability on the Petitioner's claim of ineffective assistance of trial counsel but not on the ineffective assistance of appellate counsel claim. "[J]urists of reason would find it debatable whether the [section 2255 motion] states a valid claim of the denial of a constitutional right" only related to trial counsel's performance. *Slack v. McDaniel*, 529 U.S. 473, 484 (2000); *see also* 28 U.S.C. § 2253(c)(2); *see also United States v. Winkles*, 795 F.3d 1134, 1143 (9th Cir. 2015) (explaining prisoner demonstrates substantial underlying constitutional claims under *Slack* when "reasonable jurists could debate whether ... the petition should have been resolved in a different manner or that the issues presented were adequate to deserve encouragement to proceed further.")

Dated this 15th day of December, 2022.

Honorable Cindy K. Jorgenson
United States District Judge